

(11)Publication number : 2002-271309

(43)Date of publication of application : 20.09.2002

(51)Int.Cl.

H04L 9/08  
G06F 13/00

(21)Application number : 2001-063376

(71)Applicant : SHARP CORP

(22)Date of filing : 07.03.2001

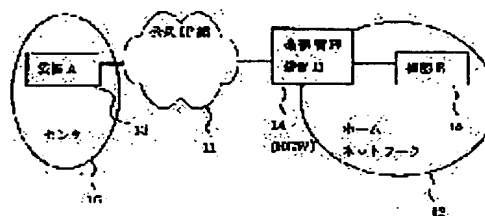
(72)Inventor : KOBAYASHI YUTAKA

(54) KEY-INFORMATION MANAGING METHOD, AND DEVICE MANAGING EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a key-information managing method and a device managing equipment wherein when a terminal outside a home network and a terminal inside the home network communicate each other, there can be eliminated the necessity of such a key exchange performed in the case of starting communication as IKE, and keys can be delivered safely to both terminals.

SOLUTION: The key-information managing method has a key AH in common between an device A 13 and an HGW 14, and has a key HB in common between the HGW 14 and the device B 15. Thus, to an access from the appliance A 13 to the device B 15, the key AH is used between the device A 13 and the HGW 14, and the key HB is used between the HBW 14 and the device B 15 as to transmit a key information AB (including a key AB) used between the devices A 13, B 15.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-271309

(P 2 0 0 2 - 2 7 1 3 0 9 A)

(43) 公開日 平成14年9月20日 (2002. 9. 20)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テマコード (参考)		
H04L 9/08		G06F 13/00	351	Z	5B089
G06F 13/00	351		357	A	5J104
	357	H04L 9/00	601	C	

審査請求 未請求 請求項の数 6 O L (全 9 頁)

(21) 出願番号 特願2001-63376 (P 2001-63376)

(22) 出願日 平成13年3月7日 (2001. 3. 7)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 小林 裕

大阪府大阪市阿倍野区長池町22番22号

シャープ株式会社内

(74) 代理人 100091096

弁理士 平木 祐輔

Fターム(参考) 5B089 GA31 GB02 KA17 KB13 KC57

KC58 KH30

5J104 AA01 AA16 EA04 EA18 NA02

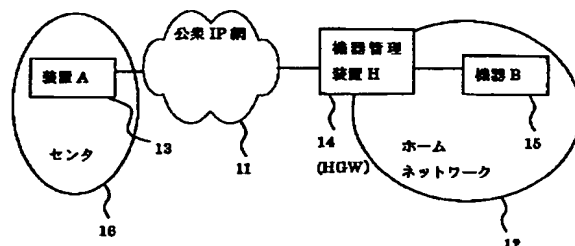
PA07

(54) 【発明の名称】 鍵情報管理方法及び機器管理装置

(57) 【要約】

【課題】 ホームネットワーク外の端末とホームネットワーク内の端末が通信を行う際に、通信をはじめる際に行われる I K E 等の鍵交換をする必要をなくすことができ、両端末に安全に鍵を配布することができる鍵情報管理方法及び機器管理装置を提供する。

【解決手段】 鍵情報管理方法は、装置 A 1 3 と H G W 1 4 との間で鍵 A H を共有するとともに、H G W 1 4 と機器 B 1 5 との間で鍵 H B を共有し、装置 A 1 3 から機器 B へのアクセスに対して、装置 A 1 3 と H G W 1 4 の間は鍵 A H を用い、H G W 1 4 から機器 B 1 5 は鍵 H B を用いて、装置 A 1 3 と機器 B 1 5 の間の鍵情報 A B (鍵 A B を含む) を伝送する。



## 【特許請求の範囲】

【請求項 1】 機器管理装置 H を介して外部ネットワークと接続される機器 B と、前記外部ネットワークに接続された装置 A との間の鍵情報管理方法であって、

前記装置 A と前記機器管理装置 H との間で鍵 A H を共有するステップと、

前記機器管理装置 H と前記機器 B との間で鍵 H B を共有するステップと、

前記機器管理装置 H では、

前記装置 A から前記機器 B へのアクセスに対して、

前記装置 A に対しては鍵 A H を用いて前記装置 A と前記機器 B の間の、鍵 A B を含む鍵情報 A B を伝送し、

前記機器 B に対しては鍵 H B を用いて前記装置 A と前記機器 B の間の、鍵 A B を含む鍵情報 A B を伝送する伝送ステップとを有することを特徴とする鍵情報管理方法。

【請求項 2】 機器管理装置 H を介して外部ネットワークと接続される機器 B と、前記外部ネットワークに接続された装置 A との間の鍵情報管理方法であって、

前記装置 A と前記機器 B のアクセスを許可するかを判断する判断ステップと、前記機器管理装置 H では、

前記判断ステップが許可と判断したときは、前記装置 A と前記機器 B とのアクセスを許可し、

前記装置 A から前記機器 B へのアクセスに対して、

前記装置 A に対しては鍵 A H を用いて前記装置 A と前記機器 B の間の、鍵 A B を含む鍵情報 A B を伝送し、

前記機器 B に対しては鍵 H B を用いて前記装置 A と前記機器 B の間の、鍵 A B を含む鍵情報 A B を伝送する伝送ステップとを有し、

前記判断ステップが否の場合には、前記伝送ステップを行わないことを特徴とする鍵情報管理方法。

【請求項 3】 前記伝送ステップでは、

前記装置 A のアドレスと前記機器 B のアドレスとその鍵 A B を含む鍵情報 A B を記録するステップと、

前記装置 A と前記機器 B の間に前記鍵情報 A B が共有できている場合に、

前記装置 A と前記機器 B が鍵 A B を用いて通信を行う際に、前記機器管理装置 H において、前記装置 A のアドレスと前記機器 B のアドレスと前記鍵情報 A B を一致するかチェックするチェックステップと、

前記チェックステップで一致しなかった場合に、パケットを破棄するステップとを有することを特徴とする請求項 2 記載の鍵情報管理方法。

【請求項 4】 少なくとも 1 個の機器 B を管理下に置き、ネットワークを介して外部の装置 A と接続された機器管理装置 H であって、

自己と装置 A との間の鍵 A H と、自己と機器 B との間の鍵 H B とを記憶する記憶手段と、

前記装置 A との間では前記鍵 A H を用い、前記機器 B に対しては前記鍵 H B を用いて、前記装置 A と前記機器 B との間の、鍵 A B を含む鍵情報 A B を伝送する伝送手段

とを備えることを特徴とする機器管理装置。

【請求項 5】 さらに、前記装置 A と前記機器 B の間のアクセスを許可するか否かを管理するテーブルを記憶するテーブル記憶手段と、

前記管理テーブルを参照し、前記装置 A と前記機器 B の通信の際に、鍵 A B を含む鍵情報 A B の伝送を制御する制御手段とを備えることを特徴とする請求項 4 記載の機器管理装置。

【請求項 6】 通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、パケットの通過を許可／不許可するパケットフィルタリング手段と、

前記パケットフィルタリングのアクセスコントロールリスト項目に、鍵 A B を含む鍵情報 A B を記憶するパケットフィルタリング記憶手段とを備え、

前記パケットフィルタリング手段は、前記アクセスコントロールリストに基づき、パケットフィルタリングを行うことを特徴とする請求項 4 記載の機器管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機器管理装置を介して外部ネットワークと接続される機器と、外部ネットワークに接続された装置との間の鍵情報管理方法及び機器管理装置に係り、特に、ネットワークにおける安全な鍵の交換が可能な鍵情報管理方法及び機器管理装置に関する。

【0002】

【従来の技術】昨今のネットワーク・システムのオープン化・汎用化により、機密情報転送や電子商取引 (Electronic Commerce) のような分野に対し、セキュリティ機能は必要不可欠なものとなっている。ネットワーク・セキュリティの目的は、ネットワークの安全保護にあり、ネットワーク・システムの機密性に応じた情報をさまざまな脅威から保護することであるとされている。一般的には、機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability)、否認拒否 (Non-Repudiation) を維持することと定義されている。一方、ネットワークに対して想定される代表的脅威としては、盗聴、漏洩、なりすまし、改ざん／偽造、不正侵入／不正アクセス、横取り、事実の否認、破壊などである。

【0003】また、ネットワーク・セキュリティのための要素技術として、秘匿・保全技術、認証技術、鍵配送技術、否認拒否技術、第三者信用機関、アクセス管理、セキュリティ監査、セキュリティ評価基準などがある。認証とは、情報通信に関与した実体 (エンティティ：人間、人間の代理として機能するプロセス、ソフトウェア、ハードウェア、通信データ等) が正当なものであるか否かを確認することであると考えられる。

【0004】一般に、ネットワークを介して端末間で通信を行うとき、脅威としてなりすましや盗聴や改ざんと

いったものがある。これらの脅威から守るための技術に、相手や送られてきたデータが正しいかを確実に確かめる認証とパケットを盗まれても情報を見ることのできないようにする暗号化がある。認証や暗号化を行うには、鍵が必要であり、その鍵を安全に交換するしくみが鍵交換である。例えば、IPv6 (Internet Protocol version6) において実装が必須となっている IPsec (Internet Protocol security) では、鍵交換で IKE (Internet Key Exchange) が規定されている。

【0005】認証には、データを送信した相手が正しいかを確かめる通信相手認証と送られてきたデータが正しいかを確認するデータ認証がある。データ認証を行う際には、2台の端末で認証データと共通鍵を用いて、一般に一方方向性ハッシュ関数を利用し相互にデータ認証を行う。通信相手認証を行うには、PKI (Public Key Infrastructure) を利用し、署名等を用いて行う。

【0006】暗号化を行う際には、送信側の端末において鍵を用いてデータを暗号化し送信する。受信側の端末においては、鍵を使いデータを復号化する。暗号化の場合には、共有鍵暗号方式と公開鍵暗号方式の2種類が知られている。共有鍵暗号方式では、送信側の端末と受信側の端末が同じ鍵を共有する方法であり、公開鍵暗号方式では、送信側の端末は受信側の端末の公開鍵を入手し暗号化を行い、受信側の端末は暗号化データを受け取ったら、自分しか知らない秘密鍵を用い復号化する方式である。

【0007】認証と暗号化のどちらの場合においても、互いに持っている鍵は安全に両者がもたなければならない。従来の技術として下記 (A) と (B) が挙げられる。

(A) 一般に、IPv6 等で実装が必須となっている IKE は鍵交換の従来技術としてよく知られている。IKE は、DH (Diffie-Hellman) を用いる。DH は、通信を行いたい2台の端末が鍵を生成するのに必要な情報を交換し、端末側で計算を行い鍵を生成するものである。このとき、できあがる共有鍵は通信路上に流れることなく、DHを行った2台の端末にしか共有鍵はわからないという利点がある。また、鍵交換のプロトコルはファイアウォールを通過するために新たなヘッダをつけるか (処理が多くなる)、ファイアウォール側で特別に穴をあけるか (セキュリティ上問題あり) する必要がある。

【0008】IPsec では、実際にパケットの中に SPI (Security Parameter Index) という領域を持っている。SPI を共有する端末は、セキュリティアソシエーション (SA) を持ち、SPI に対応する鍵やアルゴリズムの情報を保持する。SPI は、通常 IKE の手順において決定される。実際の SPI の中身は、数字のようなインデックスであって、通信路上に鍵やアルゴリズムが流れることなく、端末が SPI に対する情報 (S

A) を持つことになる。

【0009】(B) また、鍵交換を行う従来技術として、管理センタを用いる方式は特開平11-187012号公報に開示されている。管理センタを用いる方式では、まず、管理センタが、通信を行いたい2台の端末に公開鍵を配布する。管理センタの公開鍵を受けた2台の端末はそれぞれの公開鍵を管理センタに送る。管理センタは秘密値を生成し、各端末の公開鍵で暗号化して、2台の端末にそれぞれ送る。2台の端末は、それぞれ秘密値から共有鍵を計算する。この方式では、管理センタと2台の端末はそれぞれ鍵交換を行い、端末側で共有鍵の計算を行い鍵を生成する。ファイアウォールとして一般にパケットフィルタリングが知られている。これはルータ等にデフォルトで入っている機能で、従来技術では通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、決められたポリシーに基づき、パケットの通過を許可/不許可するものである。

【0010】

【発明が解決しようとする課題】しかしながら、このような従来の共有鍵交換方法にあっては、ホームネットワークにおけるセキュリティについて、以下のような問題点があった。

(A) の課題

上記したように、図1のような構成で、機器管理装置HGWを挟んだある2台の端末がセキュアな通信を始めたいとしたときにIKE等で規定されているDHを用いて鍵交換をする必要があった。鍵交換を行うときには認証処理があり、手間がかかる。また、間にファイアウォールを挟んだ場合に鍵交換プロトコルを通過させるのに手間がかかるなどの問題がある。

【0011】(B) の課題

管理センタを使い鍵を配布してもらうという方法のとき、端末側でそれぞれ鍵を計算する必要があり、端末の負担が大きい。また、2台の端末の通信時に管理センタを経由するとは限らないので、端末のホームネットワークの入り口を超えられない可能性もある。

【0012】(A) と (B) 共通の課題

また、2台の端末が間にファイアウォールを挟んで通信する場合に、暗号化されたデータ等を含むパケットがホームネットワーク内に入る際にパケットフィルタリングをするときに、アドレス等で現在行っているフィルタリングのレベルでしかできない。

【0013】End-to-Endで通信する場合に、端末側でセキュリティ関連の情報を持つ場合がある。例えば、外部の認証局とやり取りするための情報であったり、通信相手端末の証明書であったりする。End-to-Endで通信場合には、他の機関 (例えば、外部の認証局) に頼らず端末側の負担を軽くしたいが、外部の認証局等の情報、通信相手端末の証明書などを持つ必要性があり、端末の負担が大きい。また、端末側では鍵を計算することも手

間がかかるため、この負担も大きい。

【0014】本発明は、このような課題に鑑みてなされたものであって、ホームネットワーク外の端末とホームネットワーク内の端末が通信を行う際に、通信をはじめに行われるIKE等の鍵交換をする必要をなくすることができ、両端末に安全に鍵を配布することができる鍵情報管理方法及び機器管理装置を提供することを目的としている。

【0015】

【課題を解決するための手段】本発明の鍵情報管理方法は、機器管理装置Hを介して外部ネットワークと接続される機器Bと、前記外部ネットワークに接続された装置Aとの間の鍵情報管理方法であって、前記装置Aと前記機器管理装置Hとの間で鍵AHを共有するステップと、前記機器管理装置Hと前記機器Bとの間で鍵HBを共有するステップと、前記機器管理装置Hでは、前記装置Aから前記機器Bへのアクセスに対して、前記装置Aに対しては鍵AHを用いて前記装置Aと前記機器Bの間の、鍵ABを含む鍵情報ABを送送し、前記機器Bに対しては鍵HBを用いて前記装置Aと前記機器Bの間の、鍵ABを含む鍵情報ABを送送する伝送ステップとを有することを特徴としている。

【0016】本発明の鍵情報管理方法は、機器管理装置Hを介して外部ネットワークと接続される機器Bと、前記外部ネットワークに接続された装置Aとの間の鍵情報管理方法であって、前記装置Aと前記機器Bのアクセスを許可するかを判断する判断ステップと、前記機器管理装置Hでは、前記判断ステップが許可と判断したときは、前記装置Aと前記機器Bとのアクセスを許可し、前記装置Aから前記機器Bへのアクセスに対して、前記装置Aに対しては鍵AHを用いて前記装置Aと前記機器Bの間の、鍵ABを含む鍵情報ABを送送し、前記機器Bに対しては鍵HBを用いて前記装置Aと前記機器Bの間の、鍵ABを含む鍵情報ABを送送する伝送ステップとを有し、前記判断ステップが否の場合には、前記伝送ステップを行わないことを特徴としている。

【0017】また、より好ましくは、前記伝送ステップでは、前記装置Aのアドレスと前記機器Bのアドレスとその鍵ABを含む鍵情報ABを記録するステップと、前記装置Aと前記機器Bの間に前記鍵情報ABが共有できている場合に、前記装置Aと前記機器Bが鍵ABを用いて通信を行う際に、前記機器管理装置Hにおいて、前記装置Aのアドレスと前記機器Bのアドレスと前記鍵情報ABを一致するかチェックするチェックステップと、前記チェックステップで一致しなかった場合に、パケットを破棄するステップとを有することを特徴としている。

【0018】本発明の機器管理装置は、少なくとも1個の機器Bを管理下に置き、ネットワークを介して外部の装置Aと接続された機器管理装置Hであって、自己と装置Aとの間の鍵AHと、自己と機器Bとの間の鍵HBと

を記憶する記憶手段と、前記装置Aとの間では前記鍵AHを用い、前記機器Bに対しては前記鍵HBを用いて、前記装置Aと前記機器Bとの間の、鍵ABを含む鍵情報ABを送送する伝送手段とを備えることを特徴としている。

【0019】また、より好ましくは、前記装置Aと前記機器Bの間のアクセスを許可するか否かを管理するテーブルを記憶するテーブル記憶手段と、前記管理テーブルを参照し、前記装置Aと前記機器Bの通信の際に、鍵ABを含む鍵情報ABの伝送を制御する制御手段とを備えるものであってもよい。

【0020】また、通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、パケットの通過を許可／不許可するパケットフィルタリング手段と、前記パケットフィルタリングのアクセスコントロールリスト項目に、鍵ABを含む鍵情報ABを記憶するパケットフィルタリング記憶手段とを備え、前記パケットフィルタリング手段は、前記アクセスコントロールリストに基づき、パケットフィルタリングを行うものであってもよい。

【0021】

【発明の実施の形態】以下、添付図面を参照しながら本発明の好適な鍵情報管理方法及び機器管理装置の実施の形態について詳細に説明する。

第1の実施の形態

図1は、本発明の第1の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。鍵情報管理方法として、パケット通信を行うネットワークシステムに適用した例である。

【0022】図1において、11は公衆IP網、12はホームネットワーク、13は公衆IP網11を介してホームネットワーク12に接続する端末A、14はホームネットワーク12のインタフェースとなり、プロバイダ等に接続される機器管理装置（以下、HGW (Home Gateway) 又はHと略記する）、15はホームネットワーク12内で、前記HGW14を用いて通信を行う端末B、16はセンタである。

【0023】公衆IP網11のアクセス回線としてはFTTH (Fiber To The Home)、HFC (Hybrid Fiber Coax: 光同軸ケーブル)、及びADSL (Asymmetric Digital Subscriber Line) 等の大容量回線が利用可能である。ホームネットワーク12内で、HGW14を用いて通信を行う機器B15により、パケット通信を行うネットワークシステムである。ここで、装置A13はあるサービスを提供するセンタ16の端末と考えることができる。

【0024】図2は、上記機器管理装置H14の詳細な構成を示すブロック図である。図2において、機器管理装置H14は、少なくとも1個の機器Bを管理下に置き、ネットワークを介して外部の装置A13と接続され

た機器管理装置であり、オフラインで鍵AH及び鍵HBを入力する入力手段21と、自己と装置A13との間の鍵AHを記憶する鍵AH記憶手段22（記憶手段）と、自己と機器B15との間の鍵HBとを記憶する鍵HB記憶手段23（記憶手段）と、鍵AH及び鍵HBを基にデータ暗号化／復号化を行う暗号化／復号化手段24と、装置A13と機器B15の間のアクセスを許可するか否かを管理するアクセス許可／否管理テーブル25を記憶するアクセス許可／否管理テーブル記憶手段26（テーブル記憶手段）と、アクセス許可／否管理テーブル25を参照し、装置A13と機器Bの通信の際に鍵情報ABの伝送を制御するとともに、パケットフィルタリングのアクセスコントロールリスト項目に鍵情報ABを加えた形で記憶するSA（SPI）制御手段27（制御手段）と、鍵情報ABを参照したアクセスコントロールリストに基づき、パケットフィルタリングを行うパケットフィルタリング手段28と、鍵情報ABで暗号化を行って外部と通信する外部通信手段29と、鍵情報HBで暗号化を行ってホーム内で通信するホーム内通信手段30と備えて構成される。

【0025】上記外部通信手段29及びホーム内通信手段30は、全体として、装置A13と機器管理装置H14の間では鍵AHを用い、また、機器管理装置H14から機器B15に対しては鍵HBを用いて、装置A13と機器B15との間の鍵情報AB（鍵ABを含む）を伝送する伝送手段を構成している。以下、上述のように構成されたシステムの鍵情報管理方法を説明する。

【0026】図3は、ネットワークを介した鍵情報管理方法の制御シーケンスを示す図であり、装置A13、機器B15にHGW14が鍵配布を行う基本的な流れを示すフローを示す。図中、STはステップ番号を示す。図3に示すように、HGW14を挟んだ2台の装置A13、機器B15はそれぞれ事前にHGW14との間にセキュアな通信路を確保しているものとする。すなわち、ステップST1において、装置A13とHGW14は共通鍵AHを持つことによりセキュアな通信路を確保し、ステップST2において、機器B15とHGW14は共通鍵HBを持つことによりセキュアな通信路を確保している。

【0027】このときに、ステップST3で外部にある装置A13からホーム内の機器B15にアクセスしたいという要求をHGW14に送る。HGW14は、機器B15がホームの管理化にあるかどうかチェックを行い、機器B15が管理化にあると判断すれば、ステップST4で機器B15に対し装置A13のアクセスを許可するかどうかの問い合わせを送る。

【0028】ステップST5で機器B15はレスポンス24を返し、機器B15が許可すれば、ステップST6でHGW14はそれぞれのセキュアな通信路を使って共有鍵ABを装置A13と機器B15に配布する。これ以

降の、装置A13と機器B15の通信に関しては、ステップST7で共有鍵ABを用いて認証・暗号化を行い、装置A13と機器B15の間にセキュアな通信路が確保できる。

【0029】また、この2台の通信においては必ずHGW14を経由する。その際、ファイアウォールのパケットフィルタリングの際にネットワークレイヤで、あて先アドレス、送信元アドレス、ポート番号等を決められたポリシーに基づいてチェック27を行う。また、従来のアドレスやポート番号のチェックに加えて、鍵情報をチェックすることもできる（ステップST8）。

【0030】図4は、HGW14がアクセス許可／否管理テーブルを管理する場合の鍵配布の流れを示す制御シーケンスを示す図である。図1の構成で図3のようなシーケンスを行うとする。このとき、実際の一例を示したものが図4である。図3と同一処理部分には同一ステップ番号を付している。図3では、装置A13から機器B15へのアクセス要求22がHGW14にあった際に、HGW14が機器B15に対し、アクセスを許すかどうかを直接問い合わせ（ステップST4参照）している。

【0031】しかし、図4に示すように、装置A13が機器B15に対するアクセスを許すかどうかをHGW14が管理することができればこの手順は踏まなくてよく、より簡単な手順にて鍵配布が行える。HGW14は、どの端末がどの端末へのアクセスを許すかどうかのアクセス許可／否管理テーブル25を持ち、これを参照することによって実現する。すなわち、ステップST1でHGW14はアクセス許可／否管理テーブル25をチェックする。例えば、ステップST12で参照されるアクセス許可／否管理テーブル25は、装置A13から機器B15へのアクセスはOK（許可）、装置Cから機器B15へのアクセスはNG（不許可）となっている。

【0032】共有鍵ABに対する情報（鍵とアルゴリズム）もあわせて鍵配布の際に与えられる。この情報は、実際にはSPI、SAとして与えられ、装置Aと機器Bが共有鍵ABを用いて通信を行う際のパケットには必ずSPIがあり、そこに含まれる。このSPIの情報は、HGW14も2台の端末と共に共有することができ、HGW14はパケットフィルタリングの際のポリシーを作成することができる。HGW14における鍵情報のチェック（ステップST13）は、具体的にはSPIのチェックとすることができる。

【0033】次に、図2を参照して機器管理装置H（HGW）14の動作について詳細に説明する。

（装置Aと機器管理装置Hの通信）鍵情報AHは、入力手段21を用いてあらかじめオフラインで入手することができる。入力された鍵情報AHは、鍵AH記憶手段22に格納される。外部の装置Aから機器管理装置Hへの通信は、外部通信手段29で受信される。その際の通信は、鍵AHで暗号化されており、鍵情報AHを読み込

み、暗号化／復号化手段 24 を用いて復号を行う。

【0034】（機器 B と機器管理装置 H の通信）鍵情報 HB は、入力手段 21 を用いてあらかじめオフラインで入手することができる。入力された鍵情報 HB は、鍵 HB 記憶手段 23 に格納される。ホーム内の機器 B から機器管理装置 H への通信は、ホーム内通信手段 30 で受信される。その際の通信は、鍵 HB で暗号化されており、鍵情報 HB を読み込み、暗号化／復号化手段 24 を用いて復号を行う。

【0035】（機器管理装置 H から装置 A 及び機器 B への鍵情報 AB の配布）図 3 の制御シーケンスに示すように、装置 A から機器 B へのアクセス要求に対し、機器 B から了解を得られた場合に、鍵情報 AB を生成し各通信手段を用いて暗号化して通信する。また、アクセス許可／管理テーブル 25 を用いることもでき、この場合には、装置 A からのアクセス要求に対し、アクセス許可／管理テーブル 25 を参照し、鍵情報 AB を配布するか否かの判断が入る。許可された場合には前記同様の手段で鍵情報 AB の配布を行う。

【0036】（装置 A と機器 B の通信）装置 A と機器 B の通信は、鍵情報 AB を用いて暗号化される。この通信の際には、機器管理装置 H を必ず経由する（すなわち、外部通信手段 29 とホーム内通信手段 30 を通る）ので、パケットをみる事ができる。これがパケットフィルタリングの機能であり、その際に鍵情報 AB を参照し、パケットの通過の許可／不許可の決定の一役を担う。

【0037】以上説明したように、本実施の形態の鍵情報管理方法は、装置 A 13 と HGW 14 との間で鍵 AH を共有するとともに、HGW 14 と機器 B 15 との間で鍵 HB を共有し、装置 A 13 から機器 B へのアクセスに対して、装置 A 13 と HGW 14 の間は鍵 AH を用い、HGW 14 から機器 B 15 は鍵 HB を用いて、装置 A 13 と機器 B 15 の間の鍵情報 AB（鍵 AB を含む）を伝送するようにしたので、HGW 14 が外部にある装置 A とホームネットワーク内の機器 B 15 に対し安全に鍵を配布することができ、装置 A 13 から機器 B 15 と通信をはじめる際に行われる IKE 等の鍵交換をする必要がなくなる。また、装置 A 13 と機器 B 15 に安全に鍵を配布することができる。

【0038】また、HGW 14 は、オフラインで鍵 AH 及び鍵 HB を入力する入力手段 21 と、自己と装置 A 13 との間の鍵 AH を記憶する鍵 AH 記憶手段 22 と、自己と機器 B 15 との間の鍵 HB とを記憶する鍵 HB 記憶手段 23 と、暗号化／復号化手段 24 と、アクセス許可／否管理テーブル 25 を記憶するアクセス許可／否管理テーブル記憶手段 26 と、アクセス許可／否管理テーブル 25 を参照し、装置 A 13 と機器 B の通信の際に鍵情報 AB の伝送を制御するとともに、パケットフィルタリングのアクセスコントロールリスト項目に鍵情報 AB を

加えた形で記憶する SA (SPI) 制御手段 27 と、鍵情報 AB を参照したアクセスコントロールリストに基づき、パケットフィルタリングを行うパケットフィルタリング手段 28 と、鍵情報 AB で暗号化を行って外部と通信する外部通信手段 29 と、鍵情報 HB で暗号化を行ってホーム内で通信するホーム内通信手段 30 と備え、アクセス許可／否管理テーブル 25 を参照し、装置 A 13 と機器 B 15 の通信の際に鍵情報 AB の伝送を制御する。

【0039】また、装置 A 13 のアドレスと機器 B 15 のアドレスとその鍵情報 AB を、パケットフィルタリングのアクセスコントロールリストに追加する形で記憶し、装置 A 13 と機器 B 15 の間に鍵情報 AB が共有できている場合には、HGW 14 において、装置 A 13 のアドレスと機器 B 15 のアドレスと鍵情報 AB を一致するかチェックし、一致しなかった場合に、パケットフィルタリング手段 28 においてパケットを破棄するように構成したので、HGW 14 通過時のパケットフィルタリングにおいても、従来行われているアドレスやポート番号に加えて SPI もチェックすることができ、チェック項目が増えることになり、よりセキュアになる。

【0040】第 2 の実施の形態

図 5 は、第 2 の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図であり、ホームサーバにデジタル放送 TV 受信機等の情報家電機器が接続されている例である。図 5 において、41 はインターネット、42 はホームネットワーク、43 はホームネットワーク 42 内で、アドレス D により制御され HGW 46 を用いて通信を行う複数の情報家電機器 a、b、c、d、44 はセンタ、45 はインターネット 41 を介してホームネットワーク 42 に接続するセンタ端末、46 は機器管理装置 (HGW)、47 は Look up サーバ、48 はトップダウン・テストにおいて下位のモジュールが完成していない場合、暫定的に下位のモジュールの役目をするスタブ (Stub) である。

【0041】ホームネットワーク 42 内で、HGW 46 を用いて通信を行う情報家電機器 43 により、パケット通信を行うネットワークシステムである。ホームネットワーク 42 上には家庭内のあらゆる機器が接続されるとする。それらのネットワーク上のアドレスは IPv6 による 128 bit のアドレスが割り振られていて、また、それは EUI 64 アドレスを含んでいる。機器の接続はイーサネット（登録商標）、IEEE 1394、その他の手段でもかまわない。

【0042】以下、上述のように構成されたシステムの鍵情報管理方法を説明する。インターネット 41 に接続されたホームネットワーク 42 内の複数の情報家電機器 43 を、外部にあるセンタ 44 の端末 45 から制御・操作する例について考える。このとき、情報家電機器 43 を制御するミドルウェアとして Jini を用いる。Jini

は、分散オブジェクト技術であり、オブジェクト同士が非同期の通信手順を使ってメッセージのやり取りをする機能を提供するソフトウェアなどからなる。

【0043】Jiniを用いた遠隔操作の実施方法として、ホームネットワーク42内の情報家電機器43が、遠隔地より操作することのできるメソッドをスタブ48としてHGW46が持つLook upサーバ47に登録し、登録されたサービスについて遠隔地にあるセンタ44の端末45からリモートメソッドを実行し操作する。

【0044】図6は、ホームネットワークの情報家電機器の遠隔制御の制御シーケンスを示す図である。ホームネットワーク42内の情報家電機器43とHGW46は、あらかじめ、共有鍵(Key X)を用いてセキュアな通信路が確保されているものとする(ステップST20)。

【0045】まず、ステップST21でセンタ側の端末45は、ホームネットワーク42にアクセスする。ホームネットワーク42では、情報家電機器43を勝手に操作されてしまうと、火やガスを扱う機器などは人命に危害を及ぼしたり、ドアのロック等の防犯関係のものは施錠をはずしたりや異常通知をさせなかったり等の被害が考えられ、また、ホームバンキング等のものは財産に影響を及ぼしたりする。その他にも、家庭内の情報を見られてしまったりとか、他ネットワーク侵入の際の踏み台にされたりなど、ホームネットワーク42の考えられる脅威はたくさんある。こういう意味では、ホームネットワーク42というものはセキュリティがしっかりしていなければならず、HGW46は外部からのアクセスに対し、必ず認証を行う。これは、たとえばメンテナンス等の契約をしているセンタ44であってもきちんと認証の手順を踏まねばならない。この際の認証情報は、事前に持っているものとする。

【0046】事前に持つ例として、センタと契約の際に認証情報をオフライン的にHGW46がもらうことが考えられる。また、HGW46と情報家電機器43側とは自己システムであるからシステム構築時に安全に鍵情報を通知することは容易である。HGW46は認証を行い、正しいセンタと認識できた場合に、OKのレスポンスを返し(ステップST22)、センタ側端末45から公開鍵(Key A)を受け取る(ステップST23)。

【0047】センタ44は、まずホーム内の情報家電機器一覧を知る必要があり、Look upサーバ47に問い合わせを行う(ステップST24)。ステップST25でLook upサーバ47から機器の情報を得ると、リモートメソッドのスタブ48を入手する。このスタブ48を入手する際に、対象となる情報家電機器43のアドレスDや、制御したいリモートメソッドの情報がわかるステップST26。しかし、このままではアドレスDによりアクセスされる情報家電機器43とはまた認証をしないと情報家電機器43へのアクセスが許されない。

【0048】センタ側端末45は、HGW46に対し、アドレスDによりアクセスされる情報家電機器43へのアクセスを許可するかどうかの問い合わせを送る(ステップST27)。HGW46は、その問い合わせに対し、自分の管理化にアドレスDによりアクセスされる情報家電機器43があり、かつセンタ側端末45が情報家電機器43にアクセスが許されているかどうかをチェックする(ステップST28)。

【0049】これがOKならば、センタ側端末45に対しては公開鍵(Key A)を用いて共有鍵Bを暗号化して送る(ステップST29)。同様に、情報家電機器43に対しても、事前にあるセキュアな通信路50を用い、共有鍵(Key X)を用いて共有鍵Bを暗号化して送る(ステップST30)。この手順を踏むと、センタ側端末45と情報家電機器43が共有鍵(Key B)を所有することができ、それ以降の通信(センタによる情報家電機器の遠隔操作)は安全に行うことができる(ステップST31)。

【0050】このように、本実施の形態によれば、ホームネットワーク内機器B側にセンタの認証情報を持つことがなくなり、ホーム内機器側の負荷が軽くなる。機器側は、鍵の計算の手間も省け、この意味でも負担が軽くなる。なお、上記各実施の形態に係る鍵情報管理方法及び機器管理装置を、上述したようなホームネットワークの情報機器管理装置に適用することもできるが、勿論これには限定されず、暗号通信システムであれば全ての装置に適用可能である。また、上記鍵情報管理装置を構成する各手段の種類、数及び接続方法などは前述した各実施の形態に限られない。

【0051】

【発明の効果】以上、詳述したように、本発明によれば、機器管理装置が外部にある装置Aとホームネットワーク内の機器Bに対し安全に鍵を配布することができるので、装置Aから機器Bと通信をはじめる際に行われるIKE等の鍵交換をする必要がなく、装置Aと機器Bに安全に鍵を配布することができる。

【0052】機器管理装置通過時のパケットフィルタリングにおいても、従来行われているアドレスやポート番号に加えてSPIもチェックすることができ、チェック項目が増えることになり、よりセキュアになる。また、ホームネットワーク内機器B側にセンタの認証情報を持つことがなくなり、ホーム内機器側の負荷を軽くすることができる。また、機器側は、鍵の計算の手間を省くことができ、機器側においても負担を軽くすることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。

【図2】本実施の形態の鍵情報管理方法が適用されるネットワークの機器管理装置の詳細な構成を示すブロック



図である。

【図 3】本実施の形態のネットワークを介した鍵情報管理方法の制御シーケンスを示す図である。

【図 4】本実施の形態の機器管理装置がアクセス許可／否管理テーブルを管理する場合の鍵配布の流れを示す制御シーケンスを示す図である。

【図 5】第 2 の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。

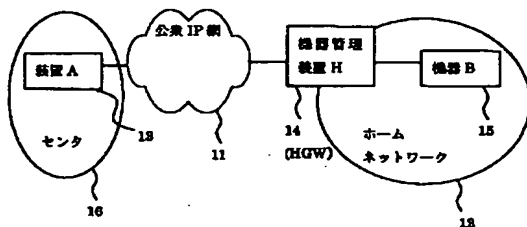
【図 6】本実施の形態のホームネットワークの情報家電機器の遠隔制御の制御シーケンスを示す図である。

【符号の説明】

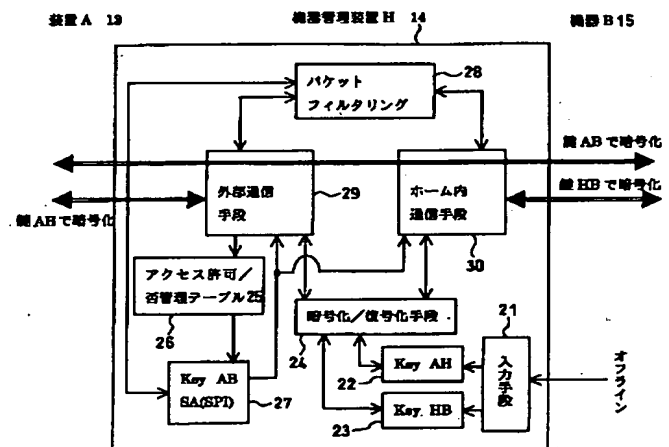
- 11 公衆 IP 網
- 12, 42 ホームネットワーク
- 13 端末 A
- 14, 46 機器管理装置 (HGW, H)
- 15 端末
- 16, 44 センタ

- 21 入力手段
- 22 鍵 AH 記憶手段 (記憶手段)
- 23 鍵 HB 記憶手段 (記憶手段)
- 24 暗号化／復号化手段
- 25 アクセス許可／否管理テーブル
- 26 アクセス許可／否管理テーブル記憶手段 (テーブル記憶手段)
- 27 SA (SPI) 制御手段 (制御手段)
- 28 パケットフィルタリング手段
- 29 外部通信手段
- 30 ホーム内通信手段
- 41 インターネット
- 43 情報家電機器
- 45 センタ端末
- 47 Lookupサーバ
- 48 スタブ (Stub)

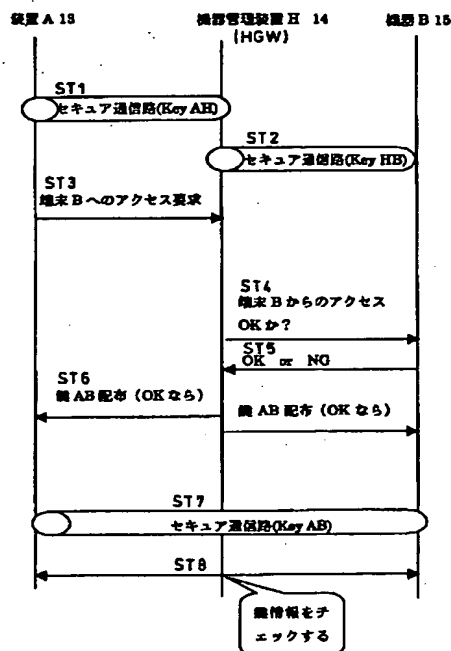
【図 1】



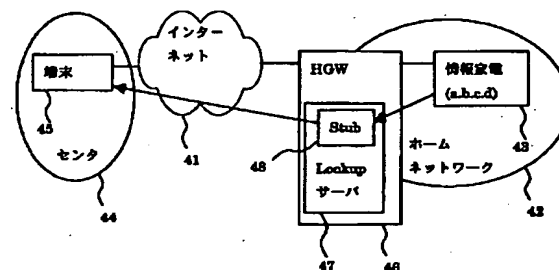
【図 2】



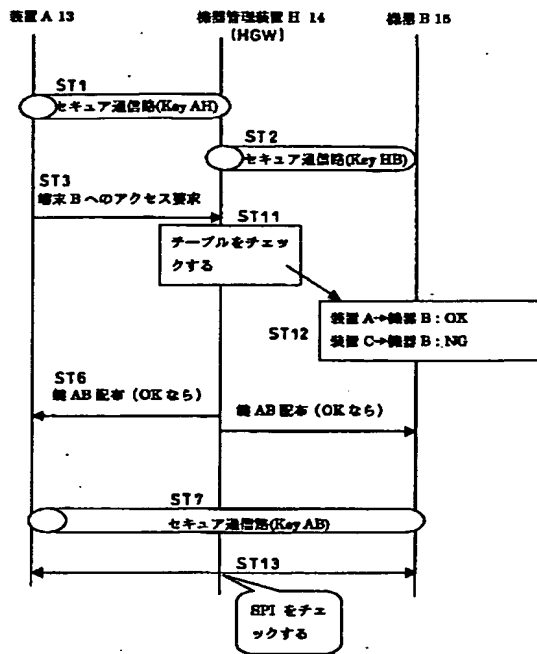
【図 3】



【図 5】



【図 4】



【図 6】

